

BIO

Versie 1



Inhoudsopgave

Voorwoord	3
DEEL 1 Achtergrond BIO	
1. Informatiebeveiliging bij de overheid	9
1.1 Inleiding	9
1.2 Informatiebeveiligingskaders en uitgangspunten overheid	9
1.3 ISO 27002	10
1.4 Evaluatie en bijstelling	11
1.5 Forum Standardisatie	11
2. Opzet van de BIO	13
2.1 Opzet BBN's	13
2.2 Controls	13
2.3 Implementatierichtlijnen	13
2.4 Overheidsmaatregelen	14
2.5 Addendum	14
2.6 Operationalisering in handreikingen	14
2.7 Rollen	14
3. Basisbeveiligingsniveaus	17
3.1 BBN1	17
3.2 BBN2	17
3.3 BBN3	18
4. Verantwoording over de BIO	19
4.1 Verantwoordelijkheid afhankelijk van basisbeveiligingsniveau	19
4.2 Explains op overheidsmaatregelen	19
4.3 Ketensamenwerking	20
4.4 Dienstenleveranciers	20
DEEL 2 Kader BIO	
Inleiding	24
BBN-toets	25
Controls en overheidsmaatregelen	26
5. Informatiebeveiligingsbeleid	27
5.1 Aansturing door de directie van de informatiebeveiliging	27
6. Organiseren van informatiebeveiliging	29
6.1 Interne organisatie	29
6.2 Mobiele apparatuur en telewerken	30
7. Veilig personeel	31
7.1 Voorafgaand aan het dienstverband	31
7.2 Tijdens het dienstverband	31
7.3 Beëindiging en wijziging van dienstverband	32
8. Beheer van bedrijfsmiddelen	33
8.1 Verantwoordelijkheid voor bedrijfsmiddelen	33
8.2 Informatieclassificatie	34
8.3 Behandelen van media	35
9. Toegangsbeveiliging	37
9.1 Bedrijfseisen voor toegangsbeveiliging	37
9.2 Beheer van toegangsrechten van gebruikers	37
9.3 Verantwoordelijkheden van gebruikers	39
9.4 Toegangsbeveiliging van systeem en toepassing	39
10. Cryptografie	41
10.1 Cryptografische beheersmaatregelen	41
11. Fysieke beveiliging en beveiliging van de omgeving	43
11.1 Beveiligde gebieden	43
11.2 Apparatuur	44
12. Beveiliging bedrijfsvoering	47
12.1 Bedieningsprocedures en verantwoordelijkheden	47
12.2 Bescherming tegen malware	48
12.3 Back-up	49
12.4 Verslaglegging en monitoren	50
12.5 Beheersing van operationele software	51
12.6 Beheer van technische kwetsbaarheden	51
12.7 Overwegingen betreffende audits van informatiesystemen	51
13. Communicatiebeveiliging	53
13.1 Beheer van netwerkbeveiliging	53
13.2 Informatietransport	54
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	55
14.1 Beveiligingseisen voor informatiesystemen	55
14.2 Beveiliging in ontwikkelings- en ondersteunende processen	56
14.3 Testgegevens	57
15. Leveranciersrelaties	59
15.1 Informatiebeveiliging in leveranciersrelaties	59
15.2 Beheer van dienstverlening van leveranciers	61
16. Beheer van informatie-beveiligingsincidenten	63
16.1 Beheer van informatiebeveiligingsincidenten en -verbeteringen	63
17. Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer	65
17.1 Informatiebeveiligingscontinuïteit	65
17.2 Redundante componenten	66
18. Naleving	67
18.1 Naleving van wettelijke en contractuele eisen	67
18.2 Informatiebeveiligingsbeoordelingen	68
Bijlage 1: Wet- en regelgeving	69
Bijlage 2: Basisbeveiligingsniveaus	70

DEEL 3 Addendum BIO		73
Inleiding Addendum		74
5. Informatiebeveiligingsbeleid	75	
5.1 Aansturing door de directie van de informatiebeveiliging	75	
6. Organiseren van informatiebeveiliging	75	
6.1 Interne organisatie	75	
7. Veilig personeel	76	
7.1 Voorafgaand aan het dienstverband	76	
7.2 Tijdens het dienstverband	76	
8. Beheer van bedrijfsmiddelen	76	
8.1 Verantwoordelijkheid voor bedrijfsmiddelen	76	
8.3 Behandelen van media	76	
11. Fysieke beveiliging en beveiliging van de omgeving	77	
11.1 Beveiligde gebieden	77	
14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	77	
14.1 Beveiligingseisen voor informatiesystemen	77	
15. Leveranciersrelaties	78	
15.1 Informatiebeveiliging in leveranciersrelaties	78	
16 Beheer van informatiebeveiligingsincidenten	78	
16.1 Beheer van informatiebeveiligings-incidenten en -verbeteringen	78	

Deel 1

Achtergrond BIO

1

Informatiebeveiliging bij de overheid

1.1 Inleiding

Informatiebeveiliging is het proces van vaststellen van de vereiste beveiliging van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen¹⁾.

De BIO beoogt zo de beveiliging van informatie (systemen) bij alle bestuurslagen en bestuursorganen van de overheid te bevorderen, zodat alle onderdelen erop kunnen vertrouwen dat onderling uitgewisselde gegevens, in lijn met wet- en regelgeving, passend beveiligd zijn. Het doel is continuïteit in de bedrijfsprocessen door waarborgen van juiste en tijdige informatie. Daarmee is de BIO ook van toepassing op besturings- en meetprocessen voor zover deze binnen een bestuursorgaan gebruikt worden.

De BIO is van toepassing op de overheid. In verband hiermee is de BIO van toepassing op de volgende bestuursorganen:

- Rijksdienst
- Provincies
- Waterschappen
- Gemeentes

Daarnaast wordt aanbevolen de BIO te verankeren in de taakomschrijving van de overige overheidsorganisaties en organisaties waarmee de overheid publiek-privaat samenwerkt en private samenwerkingen waarbij de overheid de enige aandeelhouder is.

1.2 Informatiebeveiligingskaders en uitgangspunten overheid

De overheid past risicomanagement toe om tot de juiste beveiliging van informatie en informatiesystemen te komen binnen de context van de bedrijfsdoelstellingen. Risicomanagement is het inzichtelijk en systematisch inventariseren, beoordelen en – door het treffen van maatregelen – beheersbaar maken van risico's en kansen, die het bereiken van de doelstellingen van de organisatie bedreigen dan wel bevorderen, op een zodanige wijze dat verantwoording kan worden afgelegd over de gemaakte keuzes²⁾.

1) Artikel 1 sub a Voorschrift Informatiebeveiliging Rijksdienst 2007, *Stcrt.* 2007, 122/11.

2) Artikel 5 lid 2 BVR en Artikel 1 sub d BVR.

2

Opzet van de BIO

2.1 Opzet BBN's

Om risicomanagement hanteerbaar en efficiënt te houden, kiest de BIO voor een diepgang van de uitwerking van het risicomanagement die proportioneel is aan de te beschermen belangen in combinatie met relevante dreigingen. Daarom onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). Voor BBN1 ligt de nadruk op 'wat mag minimaal verwacht worden?'. Voor BBN2 ligt de nadruk op de bescherming van de meest voorkomende categorieën informatie volgens het principe 'valt de maatregel onder goed huisvaderschap; toont deze beveiliging de betrouwbare overheid?'. BBN3²⁴⁾ is van toepassing op gerubriceerde informatie Departementaal Vertrouwelijk dan wel vergelijkbaar vertrouwelijk bij andere overheids-lagen, waarbij weerstand tegen statelijke actoren of vergelijkbare dreigers nodig is.

De keuze voor een BBN wordt gemaakt door de proceseigenaar en is gebaseerd op risicomanagement. De BIO gaat vergezeld van een methode van risicoafweging, de BBN-toets²⁵⁾. In Deel 2 wordt deze methode verder toegelicht²⁶⁾.

2.2 Controls

Na de BBN-toets doorloopt het lijnmanagement alle toepasselijke controls²⁷⁾ uit de BIO²⁸⁾. Op basis van een risicoafweging wordt bepaald hoe moet worden voldaan aan de gestelde beveiligingsdoelstellingen van de controls. Voor het voldoen aan deze doelstellingen kunnen implementatierichtlijnen uit de ISO 27002, overheidsmaatregelen en/of operationaliseren in handreikingen worden gebruikt.

Er geldt een hardheidsbepaling: in het geval een control voor een specifiek geval niet van toepassing *kan* zijn, *is* de control niet van toepassing. Dit geldt bijvoorbeeld voor een control die betrekking heeft op een externe koppeling, terwijl het betreffende informatie-systeem geen externe koppeling heeft. De organisatie hoeft zich daar niet over te verantwoorden.

2.3 Implementatierichtlijnen

Iedere control is in de ISO 27002 uitgewerkt in implementatierichtlijnen. Bij het uitvoeren van risicoafwegingen zijn de implementatierichtlijnen zeer nuttig. Ze helpen bij het kiezen van de benodigde beveiligingsmaatregelen. Deze richtlijnen moeten dus worden gezien als voorbeelden hoe de controls uitgewerkt *kunnen* worden in maatregelen; het volgen van deze richtlijnen is niet verplicht.

24) De aanvullende eisen die gelden vanaf BBN3 zijn in deze huidige versie van de BIO nog niet nader uitgewerkt.
25) De BBN-toets is geen volwaardige vervanger van de Quickcan BIO of van een andere uitgebreide risicoanalysemethodiek. De BBN-toets zorgt er alleen voor dat eenvoudig het juiste BBN geselecteerd kan worden en dat bepaald kan worden in hoeverre extra eisen noodzakelijk zijn.
26) Gewerkt gaat worden aan een handreiking waarin ten opzichte van de drie BBN-niveaus wisselingen in niveaus voor de aspecten beschikbaarheid, integriteit en vertrouwelijkheid worden aangegeven. Wellicht gaan de controls en maatregelen nog nader gespecificeerd worden naar de drie verschillende aspecten.

27) De Nederlandse versie van ISO 27002 spreekt van beheersmaatregelen. Er zijn echter ook implementatiemaatregelen. Om het onderscheid daartussen makkelijker te maken, hanteert de BIO de Engelse term, namelijk 'controls'. Het gebruik van deze term sluit aan bij de informatiebeveiligingspraktijk.
28) Met uitzondering van twee controls (6.1.4 en 14.2.4) bevat de BIO alle controls uit de ISO 27002.

■ 3

Basisbeveiligingsniveaus

Zoals in paragraaf 2.1 beschreven, onderscheidt de BIO drie basisbeveiligingsniveaus (BBN's). Ieder BBN bestaat uit een aantal controls, een aantal verplichte overheidsmaatregelen en een verantwoordings- en toezichtregime. Elk niveau bouwt voort op het vorige niveau. Daarbij vult BBN2 de controls van BBN1 aan. BBN2 vult ook de overheidsmaatregelen van BBN1 aan of vervangt deze door maatregelen met meer gewicht. Hetzelfde geldt voor BBN3 in relatie tot BBN1 en BBN2.

Als informatie wordt ontvangen van derden wordt deze ontvangen informatie behandeld conform de aanwijzingen van de afzender. Als de afzender geen markering of rubricering meegeeft wordt de ontvangen informatie behandeld conform de classificatie-eisen van het ontvangende proces.

3.1 BBN1

Informatiesystemen op BBN1 zijn systemen waarvoor BBN2 als te zwaar wordt gezien. Het kan voorkomen dat er nog wel hogere beschikbaarheids- en integriteitseisen nodig zijn. BBN1 is waar alle overheidssystemen als minimum aan moeten voldoen.

Controls en overheidsmaatregelen komen voort uit:

- wet- en regelgeving;
- algemeen geldende beveiligingsprincipes (fundamentele controls en maatregelen).

3.2 BBN2

Voor informatiesystemen binnen de overheid vormt BBN2 het uitgangspunt. BBN2 is van toepassing indien³³⁾:

- er vertrouwelijke informatie wordt verwerkt;
- mogelijke incidenten leiden tot bestuurlijke commotie;
- de veiligheid van andere systemen afhankelijk is van de veiligheid van het eigen systeem.

Het te beschermen belang van BBN2 is maximaal Departementaal Vertrouwelijk (DepV), (zoals gedefinieerd in het VIR-BI)/vergelijkbaar vertrouwelijk bij andere overheidslagen en privacygevoelige informatie met een verhoogd vertrouwelijkheidsniveau. Dergelijke informatie komt veelvuldig voor bij de overheid. Het gaat verder om commercieel vertrouwelijke informatie of informatie in het kader van beleidsvorming; het is dus niet beperkt tot als DepV/vergelijkbaar vertrouwelijk bij andere overheidslagen gerubriceerde informatie.

BBN2-informatie wordt preventief beschermd tegen alle dreigingen met uitzondering van geavanceerde dreigingen, zoals Advanced Persistent Threats (APT's), afkomstig van statelijke actoren of beroepscriminelen. Daarvoor geldt een bescherming achteraf: zij dienen te kunnen worden gedetecteerd, waarop vervolgens passend gereageerd moet worden. Voor informatiesystemen waar Departementaal Vertrouwelijke informatie en vergelijkbaar vertrouwelijk bij andere overheidslagen wordt verwerkt en waar weerstand tegen de geavanceerde dreiging van statelijke actoren of gelijkwaardige beroepscriminelen is vereist, is het BBN2 dus niet voldoende.

³³⁾ Zie de BBN-toets in Deel 2 voor meer details.

Deel 2

Kader BIO

Controls en overheidsmaatregelen

Voor de herkenbaarheid is gekozen om de nummering van de hoofdstukken en de controls in lijn te houden met de nummering uit de ISO 27002.

5

Informatiebeveiligingsbeleid

5.1 Aansturing door de directie van de informatiebeveiliging

Doelstelling: Het verschaffen van directieaansturing van en -steun voor informatiebeveiliging in overeenstemming met bedrijfseisen en relevante wet- en regelgeving.

■ 9

Toegangsbeveiliging

Algemene handreiking: [Beleid logische toegangsbeveiliging](#)

9.1 Bedrijfseisen voor toegangsbeveiliging

Doelstelling: Toegang tot informatie en informatie verwerkende faciliteiten beperken.

9.1.1	1	Beleid voor toegangsbeveiliging Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	Secretaris
9.1.2	1	Toegang tot netwerken en netwerkdiensten Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	Dienstleverancier
		Handreiking: MDM	
9.1.2.1	1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.	
9.1.2.2	1	Gebruikers met eigen of ongeauthenticeerde apparatuur (Bring Your Own Device) krijgen alleen toegang tot een onvertrouwde zone.	

9.2 Beheer van toegangsrechten van gebruikers

Doelstelling: Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot systemen en diensten voorkomen.

9.2.1	1	Registratie en afmelden van gebruikers Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	Proceseigenaar Dienstenleverancier
9.2.1.1	1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.	
9.2.1.2	1	Het gebruiken van groepsaccounts is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar.	

■ 15

Leveranciersrelaties

15.1 Informatiebeveiliging in leveranciersrelaties

Doelstelling: De bescherming waarborgen van bedrijfsmiddelen van de organisatie die toegankelijk zijn voor leveranciers.

